REMARKS/ARGUMENTS

By this Amendment, Claims 1 and 13 are cancelled, Claims 25-26 have been added and Claims 2-4, 7, 10-12, 14-19 and 21 are amended. Thus, Claims 2-12 and 14-26 are pending.

Applicants are appreciative of the courtesies extended to the undersigned by Examiner Loving during the telephonic interview on March 15, 2007.

The Examiner has rejected Claims 1-24 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,993,137 (Fransdonk) and further in view of U.S. Patent No. 5,245,656 (Loeb, et al., hereinafter "Loeb"). In particular, the Examiner asserts that Fransdonk teaches all of the features of Claim 1[1], except for obscuring the identity of the source of a message and substituting the source identification indicia with anonymous identification data that cannot be traced back to the source identification data. To make up for that deficiency, the Examiner identifies Loeb as disclosing those features and concludes that it would have been obvious for one skilled in the art to combine Fransdonk's method of secure content distribution on a network with Loeb's security method for private information delivery utilizing anonymous identification indicia to protect users. The Examiner further asserts that one skilled in the art would have been motivated to provide Fransdonk's method of secure content distribution on a network with anonymous identification indicia because it enables users to keep personal information private and untraceable.

[1] The Examiner made a similar rejection regarding the system claim, namely, Claim 13, and thus the following discussion is directed at both independent claims for the method (namely, Claim 25) and the system (namely, Claim 26).

Applicants respectfully disagree for the following reasons.

The invention of the present application is directed to a system and method for transmitting messages (which are referred to as "user activity messages") from a television end-user/subscriber terminal or device[2] to a television service network provider in **an upstream direction**. The content of these messages[3] pertain to television activities/events (e.g., what shows are being watched, how long they are being watched, channel changes, volume level change, etc.), referred to as "user activity data" which are ultimately used as part of a viewership behavior analysis by a third party. However, to protect the identity of the end user/subscriber, it is necessary to obscure or make anonymous, the end user/subscriber terminal identification. To that end, the present invention substitutes anonymous user terminal indicia for the original user terminal identification indicia in the message during the upstream transmission. As a result, the purpose of the present invention is met in that end user/subscriber activity data is passed onto a third party for analysis but without passing the end user/subscriber identity to the third party. In addition, while the television service provider can determine the end user/subscriber identification, the television service provider cannot determine the user activity data which is protected by encryption. This permits the television service provider to know whose activity is being analyzed but not anything about that underlying activity data, e.g., what shows the end user/subscriber is watching, how long they are watching, etc. Claims 1 and 13 have been cancelled and replaced by new Claims 25 and 26 to make this more clear and to more clearly distinguish over the art of record.

---

[2] Present Application, p. 7, line 29 to page 8, line 22.

In contrast, Fransdonk pertains to transmitting programming content ***from*** a programming content provider ***to*** an end-user/subscriber in what is typically described in the downstream direction. The thrust of Fransdonk is to provide a secure network for delivering content while preventing piracy of that content, i.e., protecting the content from unauthorized access. The problem that Fransdonk is concerned with is:

> ...A challenge facing traditional pay media distributors is to enable content providers to control their proprietary content, while maintaining the flexibility to distribute media content widely. The increased distribution potential heightens the need to protect and secure media content. For example, a content provider may have particular concerns regarding preventative measures to minimize the possibility of premium content falling into wrong hands, and the enforcement of copyrights. (Fransdonk, col. 1, lines 51-59)...
>
> A rapidly growing broadband Internet audience is making the Internet an exciting place to stream audio and video directly to millions of users worldwide. To overcome Internet congestion, streaming media may be pushed to the edges of the Internet (e.g., to the ISP's), where it is cached and from where the media can be streamed at high quality to the end user. Content owners are increasingly using the Internet are a platform to deliver high quality programming to a large and rapidly growing audience. However, content providers are often reluctant to put premium content on the Internet, as digital content can easily be stored, forwarded and copied without any degradation by any user with a computer and a (broadband) Internet connection. Copy protection standards, such as those specified by 5C, at the end user device using a physical secure device for decryption are expensive and somewhat unsafe. *An experienced hacker can typically break into the secure device and retrieve the decrypted content* ***and redistribute the content anonymously*** *or, in a worst-case scenario, retrieve a decryption key and* ***redistribute the content anonymously***. (emphasis added, Fransdonk, col. 2, lines 22-41)[4].

The solution proposed by Fransdonk is a method and system that basically communicates a set of session keys from content provider to content distributor to the end user for use with an encryption scheme described in detail in the Fransdonk Specification. However, in doing so, the method and system are ***not*** obscuring the identity of either the content provider or the end user,

---

[3] Present Application, p. 8, lines 10-15, as well as U.S. Patent No. 6,289,514 which is incorporated by reference.

nor would such a method/system want to do such a thing. The end user wants to receive a desired content from the content provider and the content provider wants to make certain that only the authorized end user has access to the provided content. Fransdonk makes it clear that the identity of the end user is clearly known[5].

With respect to the obscuring the identity of the content provider, this would also appear contrary to industry practice. A content provider would not want to hide its identity and it is even more likely that a television system would not be allowed to hide the identity of a content provider. The end user who is requesting the particular content would want to know that the requested content was sent by the content provider.

Loeb discloses a security system for filtering and delivering information from an information service provider over public networks. A filter station comprises end user profiles for filtering content based on the particular end user profiles. When making a request, the end user transmits its actual identity over the network to a network translator station (NTS). It is at this NTS that a pseudonym is generated which obscures the end user identity from the filter station *and from the service provider*. In contradistinction, in the present invention, the service provider can trace the actual *identity of the end user* of message but cannot know the *content* of the message.

---

[4] Per this paragraph in Fransdonk, anonymity actually works against the content provider.

[5]Fransdonk, col. 7, lines 41-57; col. 8, lines 24-27;col. 9, line 61 to col. 10, line 2; col. 10, lines 22-33; col. 10, line 55; col. 10, line 67 to col. 11, line 1; col. 11, lines 31-32; col. 17, lines 8-60; col. 18, line 17; col. 19, lines 33-40; col. 20, lines 37-45; col. 22, lines 10-26 (*trace back to end user identity*); col. 24, lines 24-34; col. 25, lines 23-40 (*trace back to end user identity*); col. 26, lines 65-67; col. 36, lines 18-24; col. 39, lines 46-59; col. 40, lines 28-33.

Since Fransdonk actually teaches away from obscuring the identity of the end user, as well as the identity of the content provider, Applicants submit that one skilled in the art would not even think of combining Fransdonk with Loeb.

Thus, for all of the above reasons, Applicants respectfully submit that Claims 25 and 26 are patentable over the art of record and request that the §103(a) rejection be withdrawn.

Claim 2 has been amended to be consistent with new Claim 25 and Claim 2 is patentable for the same reasons discussed with regard to Claim 25. The citations of Fransdonk col. 38, lines 24-33 in the Office Action are directed to a content license using a digital signature rather than anonymous ID data.

Claim 3 has been amended to be consistent with new Claim 25 and Claim 3 is dependent upon Claim 2 and is patentable for the same reasons discussed with regard to Claim 25.

Claim 4 has been amended to be consistent with new Claim 25 and Claim 4 is patentable for the same reasons discussed with regard to Claim 25. In addition, neither Fransdonk nor Loeb even mention a secure location where a viewership analysis entity cannot gain access.

Claim 5 is dependent upon Claim 4 and is patentable for the same reasons. In addition, neither Fransdonk nor Loeb even mention a viewership analysis entity obtaining access to the secure location only with assistance from a cable operator entity or agent thereof.

Claim 6 is dependent upon Claim 4 and is patentable for the same reasons. In addition, neither Fransdonk nor Loeb even mention the secure location comprising a computer that is password-protected and wherein the cable-operator entity, or an agent thereof, does not have the password.

Claim 7 is dependent upon Claim 25 and is patentable for the same reasons.

Claim 8 is dependent upon Claim 7 and is patentable for the same reasons.

Claim 9 is dependent upon Claim 7 and is patentable of the same reasons.

Claim 10 has been amended to be consistent with new Claim 25 and is patentable for the same reasons.

Claim 11 has amended to be consistent with new Claim 25 and is patentable for the same reasons.

Claim 12 has been amended to be consistent with new Claim 25 and is patentable for the same reasons.

Claim 14 has been amended to be consistent with new Claim 26 and is patentable for the same reasons. The remote device is shown in Figs. 1B, 2 and 3 of the present application. The citations of Fransdonk col. 38, lines 24-33 in the Office Action are directed to a content license using a digital signature rather than anonymous ID data.

Claim 15 has been amended to be consistent with new Claim 26 and is dependent upon Claim 14 and is patentable for the same reasons.

Claim 16 has been amended to be consistent with new Claim 26 and is dependent upon Claim 15 and is patentable for the same reasons.

Claim 17 has been amended to be consistent with new Claim 26 and is dependent upon Claim 15 and is patentable for the same reasons.

Claim 18 has been amended to be consistent with new Claim 26 and is patentable for the same reasons.

Claim 19 has been amended to be consistent with new Claim 26 and is dependent upon Claim 26 and is patentable for the same reasons. In addition, neither Fransdonk nor Loeb even mention a secure location where a viewership analysis entity cannot gain access.

Claim 20 is dependent upon Claim 19 and is patentable for the same reasons. In addition, neither Fransdonk nor Loeb even mention a viewership analysis entity obtaining access to the secure location only with the assistance from a cable operator entity or agent thereof.

Claim 21 has been amended to be consistent with new Claim 26 and is dependent upon Claim 19 and is patentable for the same reasons. In addition, neither Fransdonk nor Loeb even mention the secure location comprising a computer that is password-protected and wherein the cable-operator entity, or an agent thereof, does not have the password.

Claim 22 is dependent upon Claim 15 and is patentable for the same reasons.

Claim 23 is dependent upon Claim 22 and is patentable for the same reasons.

Claim 24 is dependent upon Claim 22 and is patentable for the same reasons.

Thus, Applicants respectfully submit that, as amended, Claims 2-12 and 14-26 are now in condition for allowance. Accordingly, prompt and favorable examination on the merits is respectfully requested.

Should the Examiner believe that anything further is desirable in order to place the application in even better condition for initial examination and allowance, the Examiner is invited to contact Applicant's undersigned attorney at the telephone number listed below.

Respectfully submitted,

CAESAR, RIVISE, BERNSTEIN,
COHEN & POKOTILOW, LTD.

May 14, 2007

By _____
Scott M. Slomowitz
Registration No. 39,032
Customer No. 03000
(215) 567-2010
Attorneys for Applicants

Please charge or credit our Account No. 03-0075 as necessary to effect entry and/or ensure consideration of this submission.